



Critical Infrastructure Centre
Cyber, Digital and Technology Policy Division
Department of Home Affairs
4 National Circuit
BARTON ACT 2600

By electronic lodgement

<https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/protecting-critical-infrastructure-systems>

16 September 2020

Protecting Critical Infrastructure and Systems of National Significance

Alinta Energy welcomes the opportunity to respond to the Department of Home Affairs consultation paper on *Protecting Critical Infrastructure and Systems of National Significance*.

Alinta Energy is an active investor in energy markets across Australia with an owned and contracted generation portfolio of nearly 3,000MW and more than 1.1 million electricity and gas customers.

We support the Government's objectives in protecting Australia's critical infrastructure and systems from emerging threats such as cyber-attacks and the recognition that achieving this across different sectors requires a flexible approach.

Regulated Critical Infrastructure Assets

The proposed 30MW threshold aligns with the Australian Energy Market Operator's threshold for registration exemption in the NEM (and 10MW in the WEM). Its purpose as a threshold is for AEMO to issue dispatch instructions and for the operation of the wholesale market in the NEM and WEM.

However, we do not believe it is of itself an appropriate threshold to define a Regulated Critical Infrastructure Asset. Numerous smaller gas-fired, distillate and biomass generators would be covered under the proposed definition, which is a significant reduction on the current thresholds set out in regulation supporting the current legislation. Such generators are geographically dispersed, operate to support the market at times of peak demand only and are not critical to the security and reliability of the NEM or WEM.

While we recognise the Government seeks to enhance security of critical infrastructure under its enhanced framework, a more proportionate approach in the electricity generation sector would be to include generation facilities that fit within the envelope of credible contingencies determined by AEMO in each region of the NEM and separately in the WEM. This approach would include generation assets that exceed the largest contingency AEMO plans for to maintain power system security. This transparent and simple approach reflects

credible disturbances that the power system is expected to withstand and would strike a balance between the cost of complying with enhanced regulatory obligations and protecting the stability and reliability of supply in the NEM and WEM.

Intermittent solar and wind generation facilities vary in size and location across the NEM and WEM. These facilities may be semi-scheduled by AEMO but are not fundamental to power system security and reliability (without significant battery storage). These facilities will also often exceed a 30MW or 10MW threshold. They may therefore be subject to additional regulatory costs without any commensurate benefit to the operation and security of power system generally. Alinta Energy would ask that the Department consult further with industry on a reasonable threshold for intermittent, variable renewable generation.

Critical Infrastructure Assets

In the Department's workshop of 27 August 2020, the proposed definition of Critical Infrastructure Assets was described as:

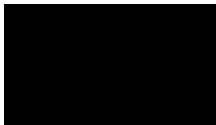
'entities involved in the production, transmission, distribution and sale of gas, electricity and liquid fuels'¹

This definition is very broad and may (unintentionally) capture a vast number of small businesses that may not be equipped to manage the compliance obligations under the enhanced regulations. For example, a small business may export small amounts of energy from a solar or biomass generator to a distribution network. Such activity has no impact on the security or reliability of the power system but may be considered critical infrastructure under the definition as it stands. Alinta Energy suggests the definition be revisited to exclude entities whose participation in the energy market is inconsequential.

Alinta Energy recognises the expectations and objectives of the Government in ensuring the legislative and regulatory framework applying to critical infrastructure and systems is fit for purpose in an environment where threats (particularly relation to cyber security) are evolving and increasingly sophisticated. At the same time, the framework needs to proportionately manage risks and threats balancing the cost of compliance and additional regulatory burdens – we acknowledge the Department is applying these considerations in its consultation.

We respond to selected questions raised in the consultation paper below and welcome further discussion with the Department on any of the matters raised in this response. Please contact David Calder (Manager, Regulatory Strategy) on [REDACTED] in the first instance.

Yours sincerely,



Graeme Hamilton

General Manager, Government & Regulatory Affairs

¹ Department of Home Affairs (2020), *Protecting Critical Infrastructure and Systems of National Significance – Energy Sector Workshop Presentation*, 27 August 2020, slide 12.

Consultation area	Question	Response
Application of the enhanced framework	2. Do you think the current definition of Critical Infrastructure is still fit for purpose?	<p>The proposed definition of critical infrastructure assets for energy is likely to be too broad (see discussion above), however we recognise the objective of government to enhance the protection of critical infrastructure and systems.</p> <p>The Australian Energy Market Operator's systems should be included due to its central role in the planning and operation of the NEM and WEM.</p>
	3. Are there factors in addition to interdependency with other functions and consequence of compromise that should be considered when identifying and prioritising critical entities and entity classes?	We understand the interdependency between gas transmission and the electricity generation sector is an issue the Department is aware of. Coal mining and rail are similarly critical to large electricity generation assets (particularly in NSW).
	4. What are the common threats you routinely prepare for and those you have faced/ experienced as a business?	<p>We prepare for:</p> <ul style="list-style-type: none"> • Terrorism; • Natural disasters (and extreme weather events); • Fire; • Protest action; • Plant and equipment failure; • Fuel supply disruptions (e.g. industry and government collaboration in the Victorian Gas Safety Case and the WA State Hazard Plan Energy Supply Disruption). • Cyber security threats to retail and wholesale information systems; • Flood and cyclone planning; • Threats to the safety of staff and the general public; and • Health pandemics (COVID-19)
	5. How should criticality be assessed to ensure the most important entities are covered by the framework?	In the energy sector, and particularly the electricity system, criticality should be determined by the importance and size of elements of the power system required to maintain reliability and system security.
	6. Which entities would you expect to be owners and operators of systems of national significance?	<p><u>For state and federal governments:</u></p> <ul style="list-style-type: none"> • Port, road, air and rail infrastructure; • Water facilities and systems; • Hospitals; • Defence infrastructure; • The Department of Home Affairs, the Australian Security and Investment Commission, the Australian Signals Directorate, the

Consultation area	Question	Response
		<p>Australian Security Intelligence Organisation and the Foreign Investment Review Board (for managing local and international cyber security threats).</p> <p><u>For statutory bodies:</u></p> <ul style="list-style-type: none"> • AEMO (as power system operator) <p><u>For the energy sector specifically:</u></p> <ul style="list-style-type: none"> • Owners and operators of large power stations (see our discussion above regarding credible contingency events and those generators who materially contribute to system security); • Significant electricity and gas transmission and distribution infrastructure; and • Refineries.
Government collaboration	7. How do you think a revised TISN and Critical Infrastructure Resilience Strategy would support the reforms proposed in this Consultation Paper?	It would improve collaboration and alignment of communications to support the reforms.
	8. What might this new TISN model look like, and what entities should be included?	A high-level, economy-wide body with representatives from government and industry and where required, sector-specific subgroups.
	9. How else should government support critical infrastructure entities to effectively understand and manage risks, particularly in relation to cross sector dependencies? What specific activities should be the focus?	<ul style="list-style-type: none"> • Understand and acknowledge the extent of other existing overlapping legislative requirements for critical infrastructure • Provide sector specific guidance on current and emerging risks and controls • Clearly map interdependencies and closely monitor risks and communicate potential issues to potential effected industries
Initiative 1: Positive Security Obligation	10. Are the principles-based outcomes sufficiently broad to consider all aspects of security risk across sectors you are familiar with?	<i>(From LYB response)</i> Principles-based outcomes are sufficiently broad, however a robust assurance and review process must also include a focus on controls assumed to be in place to mitigate the risk. Risk identification would benefit from industry sector support and guidance
	11. Do you think the security obligations strike the best balance between providing clear expectations and the ability to customise for sectoral needs?	The four categories of security obligations (physical, cyber, personnel and supply chain) support an appropriate balance between setting expectations and customisation across diverse critical infrastructure sectors.
	12. Are organisations you are familiar with already operating in-line with these principles, or do you think	In the energy sector, organisations are largely operating in-line with these principles. Additional and mandatory obligations will impose financial costs

Consultation area	Question	Response
	there would be a significant time and/or financial cost to meet these principles?	however.
	13. What costs would organisations take on to meet these new obligations?	Applying the full suite of security obligations to small entities may result in significant compliance costs. Balancing the protection of critical infrastructure and systems and focusing these on the most important elements across sectors will be the best investment of limited resources.
	14. Are any sectors currently subject to a security obligation in-line with these principles? If so, what are the costs associated with meeting this obligation? Does this obligation meet all principles, or are enhancements required? If so, what?	There are existing obligations in Victoria (through the Department of Environment, Land, Water and Planning) via its 'All Hazard' approach. It is conventional in the energy sector to maintain risk registers, hazard identification and staff training. Additional cyber security costs may be imposed under the proposed framework.
Regulators	15. Would the proposed regulatory model avoid duplication with existing oversight requirements?	As discussed above, DELWP in Victoria already has a regulatory oversight role in the energy sector for critical infrastructure. In Western Australia, Alinta Energy has obligations under the State Hazard Plan for Energy Supply disruption. See Economic regulation and consumer protection regulation is largely undertaken by the Australian Energy Regulator (in the NEM and eastern states for gas) and the Economic Regulation Authority (in WA). Streamlining any new or additional reporting and compliance obligations will reduce the cost impact to consumers and industry.
	16. The sector regulator will provide guidance to entities on how to meet their obligation. Are there particular things you would like to see included in this guidance, or broader communication and engagement strategies of the regulator?	Clear governance and guidance on expectations for reporting will be of value to industry.
	17. Who would you consider is best placed to undertake the regulatory role for sectors you are familiar with? Does the regulator already have a security-related regulatory role? What might be the limitations to that organisation taking on the role?	A single regulator would be preferred; however, we recognise in the energy sector, the functions and activities under the proposed enhancements regulating critical infrastructure are not an area that the Australian Energy Regulator (for example) is currently involved in.
	19. How can Government better support critical infrastructure entities in managing their security risks?	The Government can: <ul style="list-style-type: none"> • Keep critical infrastructure owners and operators aware of new and emerging risks; • Provide timely and clear guidance for compliance and reporting purposes; and • Minimise regulatory burden and overlap.

Consultation area	Question	Response
	21. Do you have any other comments you would like to make regarding the PSO?	Avoiding duplication in relation to positive security obligations will be an important aspect of minimise regulatory burden and cost to critical infrastructure sectors and their customers.
Initiative 3: Cyber assistance for entities	29. In what extreme situations should Government be able to take direct action in the national interest? What actions should be permissible?	If there is an imminent cyber threat or incident that could significantly impact Australia's economy, security or sovereignty
	30. Who do you think should have the power to declare such an emergency? In making this declaration, who should they receive advice from first?	The Minister, the Critical Infrastructure Centre and if necessary, the Prime Minister in collaboration with State Premiers if required.
	33. What sort of legal protections should officers (both industry and Government) undertaking emergency actions be afforded?	Owners, operators and staff of regulated infrastructure should have access to certain indemnities if following a direction from Government. For example, exemption from civil actions relating to consequences following a lawful direction.